PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-322381
(43)Date of publication of application : 24.11.2000

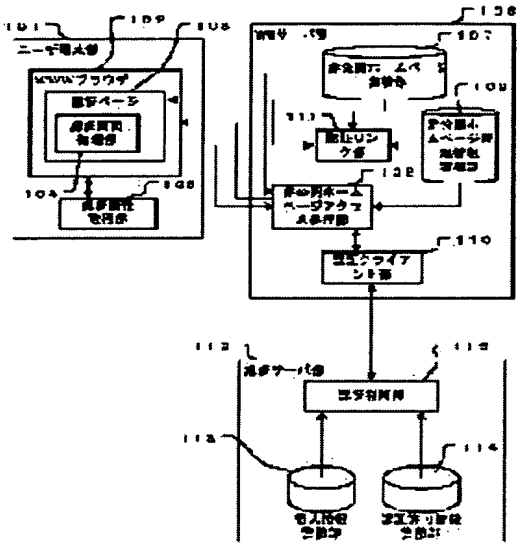
(51)Int.Cl. G06F 15/00

(21)Application number : 11-134190
(22)Date of filing : 14.05.1999

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : SUZUKI YUMIKO
NAKAMURA HIROSHI
SADAKANE TETSUO

(54) DEVICE AND METHOD FOR CONTROLLING HOMEPAGE ACCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To change authentication types in each prescribed group such as a homepage content by providing an authentication allowance information storing part in which an access control ID and an authentication type are associated and stored.
SOLUTION: In an authentication server part 112, an authentication deciding part 115 receives authentication information, an access control ID and an authentication client ID transmitted from an authentication client part 110 and detects an authentication type corresponding to a user ID, the access control ID and the authentication client ID included in the authentication information from an authentication allowance information storing part 114. The part 114 stores authentication allowance information obtained by making the access control ID correspond to the authentication type used for authentication processing. Grouping is performed by combining the user ID, the authentication client ID and the access control ID, and authentication types can be changed in accordance with the group.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－322381
（P2000－322381A）
(43)公開日　平成12年11月24日(2000.11.24)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ　５Ｂ０８５

審査請求　未請求　請求項の数３　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－134190

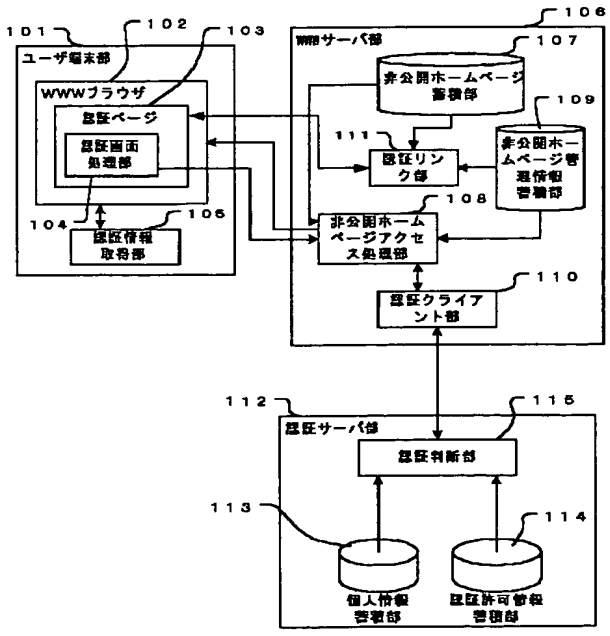
(22)出願日　平成11年５月14日(1999.5.14)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　鈴木　由美子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　中村　浩
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外２名）

最終頁に続く

(54)【発明の名称】　ホームページアクセス制御装置およびホームページアクセス制御方法

(57)【要約】
【課題】　所定グループ毎に認証種類を変えられると共に、セキュリティ性の高いホームページアクセス制御装置およびホームページアクセス制御方法を得る。
【解決手段】　ユーザ端末部とWWWサーバ部と認証サーバ部で構成され、WWWサーバ部は、グループ化された複数のホームページが蓄積された非公開ホームページ蓄積部と、ホームページのページＩＤと属するグループのアクセス制御ＩＤとが格納された非公開ホームページ管理情報蓄積部と、アクセス制御ＩＤとユーザの認証情報とを認証サーバ部に送付するアクセス部とを有し、認証サーバ部は、ユーザの認証情報が格納された個人情報蓄積部と、アクセス制御ＩＤと認証の種類とが格納された認証許可情報蓄積部と、アクセス制御ＩＤに対応する認証の種類に応じた認証情報を個人情報蓄積部から検出し、サーバ部から受け付けた認証情報とを比較して認証判断する認証判断部とを有する。



1

【特許請求の範囲】

【請求項１】　ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置において、

上記ユーザ端末部は、上記ホームページを表示するWWWブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取得した認証情報と上記ユーザ所望のホームページのページＩＤとを上記WWWサーバ部に送付する認証画面処理部とを有し、

上記WWWサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証ＯＫの場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付するアクセス部とを有し、

上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記WWWサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御ＩＤに対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記WWWサーバ部に送付する認証判断部とを有したことを特徴とするホームページアクセス制御装置。

【請求項２】　上記WWWサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御ＩＤを上記ユーザ端末に送付するように構成され、

上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページＩＤと上記アクセス部から送付されたアクセス制御ＩＤとを上記WWWサーバ部に送付するように構成され、

さらに、上記WWWサーバ部は、上記ユーザ端末部から送付された上記次のホームページのページＩＤと上記アクセス制御ＩＤとを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページＩＤに対応づけられたアクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザ端末部から送付されたアクセス制御ＩＤとを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したことを特徴とする請求項１に記載のホームページアクセス制御装置。

【請求項３】ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いたホームページアクセス制御方法において、

上記ユーザ端末部で、上記ホームページを表示するWWWブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報と上記ユーザ所望のホームページのページＩＤとを上記WWWサーバ部に送付する認証画面処理ステップとを実行し、

上記WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付けるWWW受付けステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出するWWW検出ステップと、当該WWW検出ステップで検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証ＯＫの場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末に送付するWWW送付ステップとを実行し、

上記認証サーバ部で、上記WWWサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付ける認証受付けステップと、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受付けステップで受け付けたアクセス制御ＩＤに対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記WWWサーバ部に送付する認

証送付ステップとを実行したことを特徴とするホームページアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置およびこのホームページアクセス制御装置を用いたホームページアクセス制御方法に関するものである。

【０００２】

【従来の技術】図１０は例えば、日経BP社がが発行するNECイントラネットプロジェクト編「イントラネット完全構築ガイド」(1996年)の278頁から290頁に示された従来のWWWシステムによるホームページアクセス制御装置を示す構成図である。

【０００３】図１０において、１０１はユーザ端末部、１０２はWWWブラウザ、１００１はWWWサーバ部１０６上の非公開情報（ホームページ）にアクセスするために上記WWWサーバ部１０６からユーザ端末部１０１にダウンロードされた利用者認証ページ、１００２は認証の結果に応じて上記WWWサーバ部１０６から返信された返信ホームページ、１０６はWWWサーバ部、１００３は上記WWWサーバ部１０６上で非公開情報（ホームページ）へのアクセス制御を行うアクセス制御処理部、１００４は非公開情報（ホームページ）蓄積部、１００５は利用者の認証を行う認証処理部、１００６は利用者の認証に必要な予め登録された認証情報を保持する利用者管理情報蓄積部、１００７は上記返信ホームページ１００２として公開された非公開情報（ホームページ）よりリンクされた別の非公開情報（ホームページ）を表示するリンク部である。

【０００４】次に動作について説明する。利用者がWWWサーバ部１０６上の非公開情報（ホームページ）にアクセスする際に、まず、利用者認証を行うための利用者認証ページ１００１がユーザ端末部１０１にダウンロードされ、WWWブラウザ１０２に表示される。上記利用者はこの利用者認証ページ１００１にユーザＩＤやパスワード等の予め定められた所定の認証情報を入力し、WWWサーバ部１０６に送信する。WWWサーバ部１０６では、アクセス制御処理部１００３が上記ユーザ端末部１０１から送信された上記認証情報を受け取り、認証処理部１００５に利用者の認証を依頼する。

【０００５】認証処理部１００５は利用者管理情報蓄積部１００６で保持している予め登録されたユーザＩＤやパスワード等の認証情報と、上記ユーザ端末部１０１から送信された認証情報とを照合し、利用者の認証を行い、その認証結果をアクセス制御処理部１００３に送る。アクセス制御処理部１００３は、認証結果が認証ＯＫの場合は、上記利用者が目的とする非公開情報（ホームページ）をWWWブラウザ１０２に送付し、認証ＮＧの場合はエラーメッセージ等の情報をWWWブラウザ１０２に送付し、返信ホームページ１００２として表示させる。ここで、上記返信ホームページ１００２には認証されたことを示すトークンが設定されている。上記利用者がこの返信ホームページとして表示された非公開情報（ホームページ）のリンクをたどり次の非公開情報（ホームページ）を参照する場合は、上記トークンと上記利用者が目的とする次の非公開情報（ホームページ）への指定情報とがリンク部１００７に送付される。当該リンク部１００７は、上記トークンの有効性をチェックして、有効な場合は上記指定された非公開情報（ホームページ）を返信ホームページとしてブラウザ１０２に送付し、表示させる。

【０００６】このように、従来のWWWシステムによるホームページアクセス制御装置およびその制御方法では、利用者がWWWサーバ部上の非公開情報にアクセスするときに、ユーザ端末部から送信された上記利用者の認証情報と、予め利用者管理情報蓄積部に登録された認証情報とを照合して利用者の認証を行うことにより、公開可能な利用者を限定するような制御を行うことができる。

【０００７】

【発明が解決しようとする課題】しかしながら、従来のホームページアクセス制御では、上記認証処理部は予め定められた認証の種類で認証を行うため、例えば、非公開情報（ホームページ）の内容に応じて認証の種類を変えることができないという問題があった。

【０００８】また、一度認証が行われ非公開情報（ホームページ）をアクセスすると、その非公開情報（ホームページ）からリンクが張られている次の非公開情報（ホームページ）に対して、その非公開情報（ホームページ）の内容に関わらず、新たに認証を行うことなくアクセス可能になってしまうという問題があった。

【０００９】この発明は上記のような問題点を解決するためになされたもので、例えば、ホームページの内容等の所定のグループ毎に認証の種類を変えることができると共に、キュリティ性の高いホームページアクセス制御装置およびホームページアクセス制御方法を得ることを目的とする。

【００１０】

【課題を解決するための手段】この発明に係るホームページアクセス制御装置は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置であって、上記ユーザ端末部は、上記ホームページを表示するWWWブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取

得した認証情報と上記ユーザ所望のホームページのページＩＤとを上記WWWサーバ部に送付する認証画面処理部とを有し、上記WWWサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証ＯＫの場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付するアクセス部とを有し、上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記WWWサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御ＩＤに対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記WWWサーバ部に送付する認証判断部とを有したものである。

【００１１】また、次の発明に係るホームページアクセス制御装置は、上記WWWサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御ＩＤを上記ユーザ端末に送付するように構成され、上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページＩＤと上記アクセス部から送付されたアクセス制御ＩＤとを上記WWWサーバ部に送付するように構成され、さらに、上記WWWサーバ部は、上記ユーザ端末部から送付された上記次のホームページのページＩＤと上記アクセス制御ＩＤとを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページＩＤに対応づけられたアクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザ端末部から送付されたアクセス制御ＩＤとを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したものである。

【００１２】さらにまた、次の発明に係るホームページアクセス制御方法は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いたホームページアクセス制御方法であって、上記ユーザ端末部で、上記ホームページを表示するWWWブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報と上記ユーザ所望のホームページのページＩＤとを上記WWWサーバ部に送付する認証画面処理ステップとを実行し、上記WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付けるWWW受付けステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出するWWW検出ステップと、当該WWW検出ステップで検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証ＯＫの場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末に送付するWWW送付ステップとを実行し、上記認証サーバ部で、上記WWWサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付ける認証受付けステップと、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受付けステップで受け付けたアクセス制御ＩＤに対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記WWWサーバ部に送付する認証送付ステップとを実行した方法である。

【００１３】

【発明の実施の形態】実施の形態１．以下、この発明のホームページアクセス制御装置およびホームページアクセス制御方法の実施の形態１を説明する。図１は、実施の形態１のホームページアクセス制御装置の構成を示す構成図である。図１において、１０１はユーザがホームページにアクセスするためのユーザ端末部である。１０２は上記ホームページを表示するWWWブラウザである。１０３は特定ユーザのみに公開されるホームページにアクセスするために、WWWサーバ部１０６から上記

ユーザ端末部１０１にダウンロードされ、上記WWWブラウザ１０２に表示された認証ページであり、この認証ページ１０３は上記ユーザがアクセスを所望する非公開のホームページに対応するページＩＤが設定されている。１０５は上記ユーザの認証情報を取得する認証情報取得部であり、例えば、キーボード、指紋読み取り装置等で構成され、ここでは、ユーザＩＤ、パスワード、指紋情報の認証情報を取得する。１０４は上記認証ページ１０３に定義され、上記WWWサーバ部１０６から上記ユーザ端末部１０１にダウンロードされた認証画面処理部であり、上記認証情報取得部１０５が取得した認証情報と上記ユーザ所望のホームページのページＩＤとを後述するWWWサーバ部１０６に送付する。

【００１４】１０６は上記ホームページを公開するWWWサーバ部である。１０７は所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部である。上記ホームページは例えば電子ファイルでなる。１０９は上記複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部であり、ここでは、さらに上記非公開ホームページ蓄積部１０７にホームページが存在するパス名が上記ホームページのページＩＤに対応づけられて格納されている。

【００１５】１０８は上記ユーザ端末部１０１の認証画面処理部１０４から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部１０９から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザの認証情報とを後述する認証クライアント部１１０に送付して認証要求し、当該認証結果が認証ＯＫの場合に上記非公開ホームページ管理情報蓄積部１０９から上記ページＩＤに対応づけられたパス名を検出し、当該検出したパス名に従って上記非公開ホームページ蓄積部１０７から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付する非公開ホームページアクセス処理部である。また、ここでは上記ユーザ端末１０１にホームページを送付する際に、当該ホームページが属するグループのアクセス制御ＩＤを含む認証を保証するトークンを上記ユーザ端末１０１に送付するように構成されている。

【００１６】１１０は上記非公開ホームページアクセス処理部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け取り、当該アクセス制御ＩＤ、ユーザの認証情報および認証クライアントＩＤを後述する認証サーバ部１１２に送付して認証要求し、当該認証結果を上記認証サーバ部１１２から受け取って上記非公開ホームページアクセス処理部１０８に送付する認証クライアント部である。上記認証クライアントＩＤは認証クライアント部を識別するＩＤである。例えば、WWWサーバ部が複数ある場合は上記認証クライアント部も複数存在するため、認証クライアントＩＤにより複数のWWWサーバを区別することができ、有効である。また、本実施の形態では、上記非公開ホームページアクセス処理部１０８と上記認証クライアント部１１０でアクセス部を構成する。

【００１７】１１１は上記ユーザ端末部１０１から送付された上記次のホームページのページＩＤと上記アクセス制御ＩＤを含む上記トークンとを受け付け、上記非公開ホームページ管理情報蓄積部１０９から上記次のホームページのページＩＤに対応づけられたアクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザ端末部１０１から送付された上記トークンに含まれたアクセス制御ＩＤとを比較すると共に、上記トークンの有効性を判断し、有効である場合に上記非公開ホームページ管理情報蓄積部１０９から上記ページＩＤに対応づけられたパス名を検出し、当該検出したパス名に従って上記非公開ホームページ蓄積部１０７から上記次のホームページを検出して上記ユーザ端末部１０１に送付する認証リンク部である。

【００１８】１１２は上記ホームページをアクセスするユーザの認証を行う認証サーバ部である。１１３は上記ユーザの予め登録された認証情報を含むユーザ情報が格納された個人情報蓄積部である。１１４は上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部である。上記WWWサーバ部１０６の認証クライアント部１１０から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部１１４から上記アクセス制御ＩＤに対応づけられた認証の種類を検出し、上記個人情報蓄積部１１３から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記認証クライアント部１１０から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記認証クライアント部１１０に送付する認証判断部である。

【００１９】次に、ホームページアクセス制御装置の動作およびホームページアクセス制御方法について説明する。ユーザは、特定ユーザのみに公開される所望のホームページにアクセスする際に、例えば、ユーザ端末部１０１に所定のＵＲＬを入力すると、上記ユーザ所望のホームページに対応するページＩＤが設定された認証ページ１０３が、上記WWWサーバ部１０６から上記ユーザ端末部１０１にダウンロードされる。そして上記認証ページ１０３に定義された認証画像処理部１０４がWWWブラウザ１０２に認証画面を表示する。

【００２０】図２は、上記認証画面処理部１０４が表示する画面の一例である。図２の画面では、上記ユーザは

認証情報としてユーザＩＤ、パスワード、指紋情報（指１本）、指紋情報（指２本）が選択可能である。

【００２１】上記ユーザは、上記WWWブラウザ１０２に表示された認証画面を確認し、必要な認証項目を選択して、認証情報を入力する。例えば、ユーザＩＤやパスワードは、キーボードより入力し、指紋情報は、上記認証画面処理部１０４が表示した認証画面の取得ボタンを押下して入力する。また、例えば、認証情報取得部１０５に接続されたＩＣカード読み取り装置に、ユーザＩＤ、パスワード、指紋情報等が記録されたＩＣカードを読み取らせることにより、上記認証情報を入力する。

【００２２】上記ユーザの入力操作に応じて、認証情報取得部１０５は、上記ユーザの認証情報を取得する（認証情報取得ステップ）。例えば、上記キーボードから入力されたキーコードをユーザＩＤやパスワードの認証情報として取得する。また、上記認証画面処理部１０４の取得ボタンの位置に設置された指紋読み取り装置のセンサーが上記ユーザの押下を指紋情報として取得する。さらにまた、上記ＩＣカード読み取り装置が上記ユーザのＩＣカードに記憶されていたユーザＩＤ、パスワード、指紋情報等を読み取り、認証情報として取得する。

【００２３】その後、上記ユーザが上記認証画面に表示された送信ボタンを押下すると、上記認証画面処理部１０４が、上記認証情報取得部１０５によって取得された認証情報と、上記認証ページ１０３に設定されていたページＩＤとを上記WWWサーバ部１０６上の非公開ページアクセス処理部１０８に送付する（認証画面処理ステップ）。すると、上記非公開ページアクセス処理部１０８は、上記認証情報とページＩＤを受け取り、認証処理を開始する。

【００２４】以降の非公開文書アクセス処理部１０８の詳細な動作および処理について図１、図３および図４を用いて説明する。

【００２５】図３は、非公開ホームページ管理情報蓄積部１０９に格納されたデータの一例である。図３において、３０１はホームページを識別するページＩＤである。３０２はホームページが属するグループを識別するアクセス制御ＩＤであり、ここでは上記ホームページは内容によってグループ化されている。３０３はホームページが存在する場所（パス名）である。図３では、５つのホームページのそれぞれのページＩＤ、アクセス制御ＩＤおよびパス名が格納されている。また、図４は、非公開ホームページアクセス処理部１０８の動作を示す流れ図である。

【００２６】非公開文書アクセス処理部１０８は、まず上記認証画面処理部１０４より送付された上記ユーザの認証情報と上記ユーザ所望の非公開ホームページのページＩＤとを受け付ける（ステップ４０１、WWW受付けステップ）。そして非公開ホームページ管理情報蓄積部１０９より、上記受け取ったページＩＤに対応づけられたアクセス制御ＩＤを検出し取得する（ステップ４０２、WWW検出ステップ）。次にこのアクセス制御ＩＤと上記ユーザの認証情報とを認証クライアント１１０に送付して認証処理を依頼する（ステップ４０３、認証要求ステップ）。

【００２７】そして、上記認証クライアント１１０から送付された認証結果がＯＫであるか否かを判断する（ステップ４０４）。認証結果が認証ＯＫの場合は、非公開ホームページ管理情報蓄積部１０９よりページＩＤに対応づけられたホームページが存在するパス名を検出し、当該検出したパス名に従って非公開ホームページ蓄積部１０７よりホームページを検出してWWWブラウザ１０２にそのホームページを送付する（ステップ４０５、WWW送付ステップ）。一方、認証結果がＯＫではなかった場合、すなわち認証ＮＧであった場合は、エラーメッセージ用のホームページをWWWブラウザ１０２に送付する（ステップ４０６）。このように、認証が成功した場合は、上記ユーザ所望の非公開ホームページがWWWブラウザ１０２に表示されるが（WWWブラウザステップ）、認証が失敗した場合は、認証エラー、認証方法エラー等のエラーメッセージがWWWブラウザ１０２に表示され、上記ユーザは、非公開ホームページへアクセスすることができない。

【００２８】次に、上記認証処理の詳細な動作および処理について図１、図５および図６を用いて説明する。図５は、個人情報蓄積部１１２に格納された認証情報を含む個人情報の一例である。図５では、認証情報としてユーザＩＤ、パスワード、指紋１本の情報、指紋２本の情報が格納されると共に、個人名称、所属、連絡先等の個人情報も格納されている。尚、ここでは、ユーザＩＤが個人情報のキーである。

【００２９】図６は、認証許可情報蓄積部１１４に格納されたアクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられた認証許可情報の一例であり、ここでは、上記アクセス制御ＩＤのほかに、ユーザＩＤおよび認証クライアントＩＤが格納され、上記アクセス制御ＩＤ、ユーザＩＤおよび認証クライアントＩＤの組み合わせに応じて認証に用いられる認証の種類が決定されるようになっている。

【００３０】図６において、６０１は非公開ホームページをアクセスするユーザのユーザＩＤ、６０２は認証クライアント部１１０を識別する認証クライアントＩＤ、６０３は上記ユーザ所望のホームページのグループを識別するアクセス制御ＩＤ、６０４はユーザＩＤのユーザが認証クライアントＩＤの認証クライアントでアクセス制御ＩＤに対するアクセス権を認証するときの認証手段、すなわち認証の種類、６０５は備考である。

【００３１】図６の例では、user1がAclientでJINJI1に対してアクセスする時は、ユーザＩＤと指紋１本の情報で認証すること、user1がAclientでKEIRI1に対してアク

セスする時は、ユーザＩＤとパスワード情報で認証することが定義されている。すなわちこの例では、ユーザＩＤ６０１、認証クライアントＩＤ６０２およびアクセス制御ＩＤ６０３の組合わせによってグループ化し、そのグループに応じて認証の種類を変えることが可能となる。

【００３２】まず、認証判断部１１５は、上記認証クライアント部１１０より送付された上記認証情報、上記アクセス制御ＩＤおよび上記認証クライアントＩＤを受け付け（認証受付けステップ）、認証許可情報蓄積部１１４から上記認証情報に含まれるユーザＩＤ、上記アクセス制御ＩＤおよび上記認証クライアントＩＤに対応する認証の種類を検出する。そして、上記認証許可情報蓄積部１１４から検出された認証の種類に応じた認証情報を上記ユーザＩＤをキーとして上記個人情報蓄積部１１３から検出する（認証検出ステップ）。次に、上記個人情報蓄積部１１３から検出された認証情報と上記認証クライアント部１１０より受け付けた認証情報とを比較して、上記ユーザの認証を行い（認証判断ステップ）、その結果を上記認証クライアント部１１０に送付する（認証送付ステップ）。ここで、上記個人情報蓄積部１１３から検出した認証情報と上記認証クライアント部１１０より渡された認証情報とが一致する場合は、認証結果として認証ＯＫを送付し、一致しない場合は、認証ＮＧを送付する。

【００３３】次に、WWW装置の全体の動作を説明する。図７は、認証処理の全体の流れを示すシーケンス図である。まず、ユーザが、特定ユーザのみに公開される所望のホームページにアクセスするために、上記所望のホームページに対応するＵＲＬをユーザ端末部１０１に入力すると、WWWサーバ部１０６から上記ユーザ所望のホームページに対応するページＩＤと認証画像処理部１０４の設定された認証ページ１０３が上記ユーザ端末部１０１に送付される。

【００３４】その後、上記認証画面処理部１０４は、上記ユーザより入力された認証情報と上記認証ページ１０３に設定された上記ユーザ所望のホームページに対応するページＩＤとを、非公開ホームページアクセス処理部１０８に送付する（シーケンス７０１）。すると、上記非公開ホームページアクセス処理部１０８は、非公開ホームページ管理情報蓄積部１０９より上記ページＩＤに対するアクセス制御ＩＤを検出し、当該アクセス制御ＩＤと上記ユーザより入力された認証情報とを認証クライアント１１０に送付し、認証を依頼する（シーケンス７０２）。

【００３５】当該認証クライアント部１１０は、認証プロトコルに従って認証判断部１１５に認証を依頼すると共に、上記非公開ホームページアクセス処理部１０８から送付されたアクセス制御ＩＤ、認証情報および該認証クライアント部１１０に対応する認証クライアントＩＤを認証判断部１１５に送付する（シーケンス７０３）。当該認証判断部１１５は、個人情報蓄積部１１３と認証許可情報蓄積部１１４の情報を用いて認証を行い、認証ＯＫか認証ＮＧかの認証結果を認証クライアント部１１０に送付する（シーケンス７０４）。

【００３６】上記認証結果を受け取った認証クライアント部１１０は、その結果を更に上記非公開ホームページアクセス処理部１０８に送付する（シーケンス７０５）。当該非公開ホームページアクセス処理部１０８は、上記認証結果が認証ＮＧの場合は、エラーメッセージ用のホームページをWWWブラウザ１０２に送付し、認証結果がＯＫの場合は、非公開ホームページ管理情報蓄積部１０９より上記ページＩＤに対するホームページの存在パス名を検出し、そのそのパス名に従って非公開ホームページ蓄積部１０７より上記ホームページを検出し、WWWブラウザ１０２に送付する。尚、このとき、このホームページからリンクされた次のホームページをアクセスするために、認証を保証する上記アクセス制御ＩＤを含むトークンをこのホームページに設定しておく（シーケンス７０６）。

【００３７】次に認証リンク部１１１の詳細動作および処理について、図８を用いて説明する。図８は、上記認証リンク部１１１の詳細な動作を示す流れ図である。前述のようにして認証ＯＫとなり、上記ユーザ所望のホームページが上記WWWブラウザ１０２に表示された後、上記ユーザが上記ユーザ所望のホームページからリンクされた次のホームページをアクセスすると、上記認証リンク部１１１は、アクセス要求として上記WWWブラウザ１０２から送付された上記表示されたホームページに設定されたトークンと、上記ユーザ所望の次のホームページに対応したページＩＤとを受け付ける。（ステップ８０１）。

【００３８】そして、上記認証リンク部１１１は、暗号化されているトークンの暗号を解きトークンの有効性の確認する（ステップ８０２）。上記トークンは、例えば、先に認証ＯＫとなった時刻、認証ＯＫとなったアクセス制御ＩＤ、有効性判定用の固定値等の情報を含み、当該各情報が有効と判断された場合にトークンの有効性を満足する。

【００３９】次に、上記認証リンク部１１１は、上記トークンが有効であるか否かを判断し（ステップ８０３）、上記トークンが無効な場合は、アクセスエラーを表示するホームページを上記WWWブラウザ１０２に送付する（ステップ８０５）。一方、上記トークンが有効な場合は、上記ユーザ所望の次の非公開ホームページに対応したページＩＤに対するアクセス制御ＩＤを上記非公開ホームページ管理情報蓄積部１０９より検出する（ステップ８０４）。そして、当該非公開ホームページ管理情報蓄積部１０９より検出したアクセス制御ＩＤと、上記トークンに含まれていた認証時のアクセス制御

ＩＤとの比較を行う（ステップ８０６）。

【００４０】ステップ８０６で比較した結果、違っていた場合は、アクセスエラーを表示するホームページを上記WWWブラウザ１０２に送付し（ステップ８０５）、認証は継続されない。一方、ステップ８０６で比較した結果、同じであった場合は、認証が継続され、上記認証リンク部１１１は、上記非公開ホームページ管理情報蓄積部１０９から検出したページＩＤの存在パス名に従って上記非公開ホームページ蓄積部１０７よりホームページを検出し、新たなトークンを設定して、上記WWWブラウザ１０２に送付する（ステップ８０８）。このように、アクセス制御ＩＤが一致した場合は、認証が継続され、新たに認証を行うことなく次のホームページにアクセスることが可能であるが、トークンが無効である又はアクセス制御ＩＤが一致しない場合は、認証は継続されず、例えば、新たに認証を行い、認証ＯＫとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることができる。

【００４１】図９は、特定ユーザのみに公開されるホームページをリンクをたどりながらアクセスしていく時のシーケンス図である。まず、前述のように、ユーザが所望のホームページに対応したＵＲＬを入力すると、上記ホームページのページＩＤと認証画面処理部１０４とが設定された認証ページ１０３がユーザ端末部１０１にダウンロードされる。そして、上記認証画面処理部１０４はユーザより入力された認証情報と上記認証ページ１０３に設定されているページＩＤとを、非公開ホームページアクセス処理部１０８に送付する（シーケンス７０１）。

【００４２】当該非公開ホームページアクセス処理部１０８は、非公開ホームページ管理情報蓄積部１０９より上記送付されたページＩＤに対するアクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記送付された認証情報とを認証クライアント１１０に送付し認証処理を依頼する（シーケンス９０１）。その結果、認証ＯＫの場合、上記非公開ホームページアクセス処理部１０８は、非公開ホームページ蓄積部１０６より該当するホームページを検出し（シーケンス９０２）、認証を保証するアクセス制御ＩＤを含むトークン（トークン１）を生成し（シーケンス９０３）、上記検出したホームページに設定してWWWブラウザ１０２に送付する（シーケンス９０４）。図９では、ページＩＤがpage1のホームページに対して、page1.htmlの電子ファイルの内容を送付している。

【００４３】次に、page1.htmlからのリンクによりページＩＤがpage2であるホームページへのアクセス依頼が認証リンク部１１１に届く。このときpage1.htmlに設定されていたトークン（トークン１）も送付される（シーケンス９０５）。すると、認証リンク部１１１は、上記トークンを解読して（シーケンス９０６）トークンの有効性を確認する。そしてpage2のアクセス制御ＩＤとトークン１に含まれるアクセス制御ＩＤ、すなわちpage1のアクセス制御ＩＤをチェックして、上記page1のアクセス制御ＩＤと上記page2のアクセス制御ＩＤの継続性を確認する（シーケンス９０７）。上記page1とpage2のアクセス制御ＩＤが一致し、トークンに異常がない場合は、上記page2のホームページを非公開ホームページ蓄積部１０７より検出し（シーケンス９０８）、新たなトークン（トークン２）を生成する（シーケンス９０９）。そして、上記page2のホームページの電子ファイルであるpage2.html に上記生成したトークンを設定してWWWブラウザ１０２に送付する（シーケンス９１０）。

【００４４】以上のように本実施の形態によれば、複数のホームページが当該ホームページの内容に応じてアクセス制御ＩＤによりグループ化され、該アクセス制御ＩＤと認証に用いられるユーザＩＤ、パスワード、指紋情報などの認証の種類とが対応づけられて格納された認証許可情報蓄積部を用いたことにより、アクセス可能なユーザかの認証判断を行う際に、上記グループのアクセス制御ＩＤに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御ＩＤに応じて認証の種類が決定されるので、例えば、複数のWWWサーバ部に複数のホームページがそれぞれ存在する場合でも、上記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となる。

【００４５】また、上記認証許可情報蓄積部が、上記アクセス制御ＩＤ、ユーザＩＤおよび認証クライアントＩＤの組み合わせに応じて認証に用いられる認証の種類が決定されることにより、より詳細にグループを分類することができるので、システム運用形態に応じてより適切な認証の種類で認証判断を行うことが可能となる。

【００４６】また、非公開ホームページアクセス処理部がユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御ＩＤを上記ユーザ端末に送付し、認証リンク部が上記アクセス制御ＩＤと上記ホームページにリンクされたユーザ所望の次のホームページのアクセス制御ＩＤとを比較して認証の継続を判断し、一致する場合、すなわち認証が継続している場合に上記次のホームページを上記ユーザ端末部に送付することにより、ユーザが別のホームページをアクセスする度に上記ユーザの認証情報による認証を行う必要がないため、ユーザの操作性を向上することが可能となる。また、トークンが無効である又はアクセス制御ＩＤが一致しない場合、すなわち先に認証ＯＫとなったアクセス制御ＩＤと異なるアクセス制御ＩＤに属するホーム

ページをアクセスする場合は、認証は継続していないとし、例えば、新たに認証を行い、認証ＯＫとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることが可能となる。

【００４７】なお、本実施の形態では、認証判断部が個人情報蓄積部を検出する際にユーザＩＤをキーとしたが、上記キーは、ユーザを一意に決定できるものであれば良く、上記ユーザＩＤに限定されるものではない。例えば、認証クライアント部から送付されたユーザＩＤが未定義であっても、ユーザを一意に決定できる指紋情報からまずユーザＩＤを確定した後、同様の処理を行うことも可能である。

【００４８】

【発明の効果】以上のように、この発明のホームページアクセス制御装置によれば、ホームページを公開するＷＷＷサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるものにおいて、上記ユーザ端末部は、上記ホームページを表示するＷＷＷブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取得した認証情報と上記ユーザ所望のホームページのページＩＤとを上記ＷＷＷサーバ部に送付する認証画面処理部とを有し、上記ＷＷＷサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証ＯＫの場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付するアクセス部とを有し、上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記ＷＷＷサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御ＩＤに対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記ＷＷＷサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記ＷＷＷサーバ部に送付する認証判断部とを有したことにより、アクセス可能なユーザかの認証判断を行う際に、上記グループのアクセス制御ＩＤに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御ＩＤに応じて認証の種類が決定されるので、例えば、複数のＷＷＷサーバ部に複数のホームページがそれぞれ存在する場合でも、上記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となるという効果がある。

【００４９】また、次の発明のホームページアクセス制御装置によれば、上記ＷＷＷサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御ＩＤを上記ユーザ端末に送付するように構成され、上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページＩＤと上記アクセス部から送付されたアクセス制御ＩＤとを上記ＷＷＷサーバ部に送付するように構成され、さらに、上記ＷＷＷサーバ部は、上記ユーザ端末部から送付された上記次のホームページのページＩＤと上記アクセス制御ＩＤとを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページＩＤに対応づけられたアクセス制御ＩＤを検出し、当該検出したアクセス制御ＩＤと上記ユーザ端末部から送付されたアクセス制御ＩＤとを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したことにより、アクセス制御ＩＤが一致しない場合、すなわち先に認証ＯＫとなったアクセス制御ＩＤと異なるアクセス制御ＩＤに属するホームページをアクセスする場合は、例えば、新たに認証を行い、認証ＯＫとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることが可能となるという効果がある。また、アクセス制御ＩＤが一致した場合は、ユーザが別のホームページをアクセスする度に上記ユーザの認証情報による認証を行う必要がないため、ユーザの操作性を向上することが可能となるという効果がある。

【００５０】さらにまた、次の発明のホームページアクセス制御方法によれば、ホームページを公開するＷＷＷサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いた制御方法において、上記ユーザ端末部で、上記ホームページを表示するＷＷＷブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報

と上記ユーザ所望のホームページのページＩＤとを上記WWWサーバ部に送付する認証画面処理ステップとを実行し、上記WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページＩＤと上記ユーザの認証情報とを受け付けるWWW受付けステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページＩＤと上記ホームページがそれぞれ属するグループのアクセス制御ＩＤとが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページＩＤに対応づけられた上記アクセス制御ＩＤを検出するWWW検出ステップと、当該WWW検出ステップで検出したアクセス制御ＩＤと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証ＯＫの場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末に送付するWWW送付ステップとを実行し、上記認証サーバ部で、上記WWWサーバ部から送付された上記アクセス制御ＩＤと上記ユーザの認証情報とを受け付ける認証受付けステップと、上記アクセス制御ＩＤと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受付けステップで受け付けたアクセス制御ＩＤに対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記WWWサーバ部に送付する認証送付ステップとを実行したことにより、アクセス可能なユーザかの認証判断を行う際に、上記グループのアクセス制御ＩＤに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御ＩＤに応じて認証の種類が決定されるので、例えば、複数のWWWサーバ部に複数のホームページがそれぞれ存在する場合でも、上

記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となるという効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１によるホームページアクセス制御装置を示す構成図である。

【図２】　この発明の実施の形態１において認証画面処理部が表示する画面の一例を示す説明図である。

【図３】　この発明の実施の形態１において非公開ホームページ管理情報蓄積部に格納されたデータの一例を示す説明図である。

【図４】　この発明の実施の形態１における非公開ホームページアクセス処理部の詳細動作を示す流れ図である。

【図５】　この発明の実施の形態１において個人情報蓄積部に格納されたデータの一例を示す説明図である。

【図６】　この発明の実施の形態１において認証許可情報蓄積部に格納されたデータの一例を示す説明図である。

【図７】　この発明の実施の形態１における認証処理の流れを説明するシーケンス図である。

【図８】　この発明の実施の形態１における認証リンク部の詳細動作を示す流れ図である。

【図９】　この発明の実施の形態１において非公開ホームページのリンクをたどったアクセスの制御の流れを示すシーケンス図である。

【図１０】　従来のホームページアクセス制御装置を示す構成図である。

【符号の説明】

１０１：ユーザ端末部、１０２：WWWブラウザ、１０３：認証ページ、１０４：認証画面処理部、１０５：認証情報取得部、１０６：WWWサーバ部、１０７：非公開ホームページ蓄積部、１０８：非公開ホームページアクセス処理部、１０９：非公開ホームページ管理情報蓄積部、１１０：認証クライアント部、１１１：認証リンク部、１１２：認証サーバ部、１１３：個人情報蓄積部、１１４：認証許可情報蓄積部、１１５：認証判断部

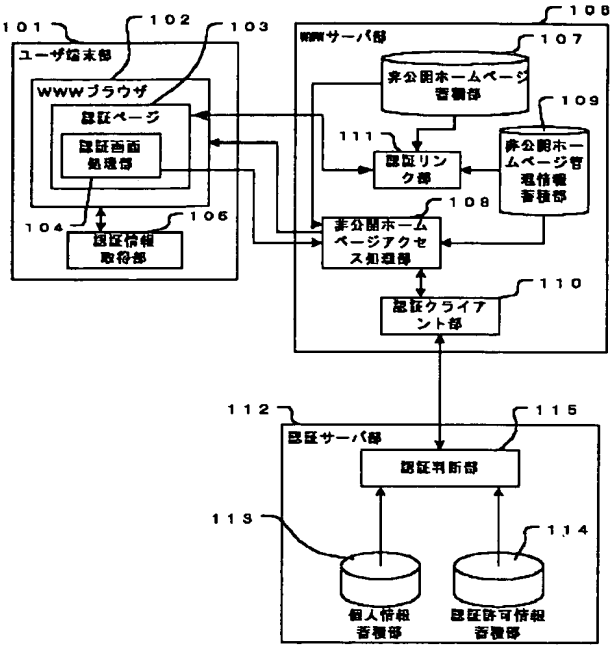
【図３】

301 ページID	302 アクセス制御ID	303 ホームページが存在するパス名
page1	JINJI1	C:¥JINJI1¥page1.html
page2	JINJI1	C:¥JINJI1¥page2.html
Page3	JINJI1	C:¥JINJI¥page3.html
page4	KEIRI1	C:¥KEIRI1¥page4.html
page5	KEIRI1	C:¥KEIRI1¥page5.html

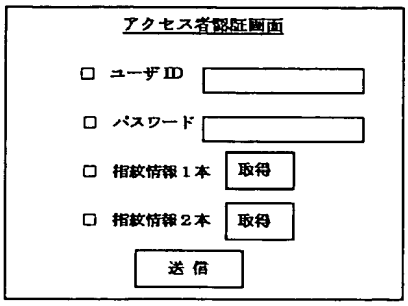
【図５】

ユーザID	パスワード	指紋情報１	指紋情報２	個人名称	所属	……
user1	user1pass	指紋情報へのポインタ	指紋情報へのポインタ	認証花子	経理	……

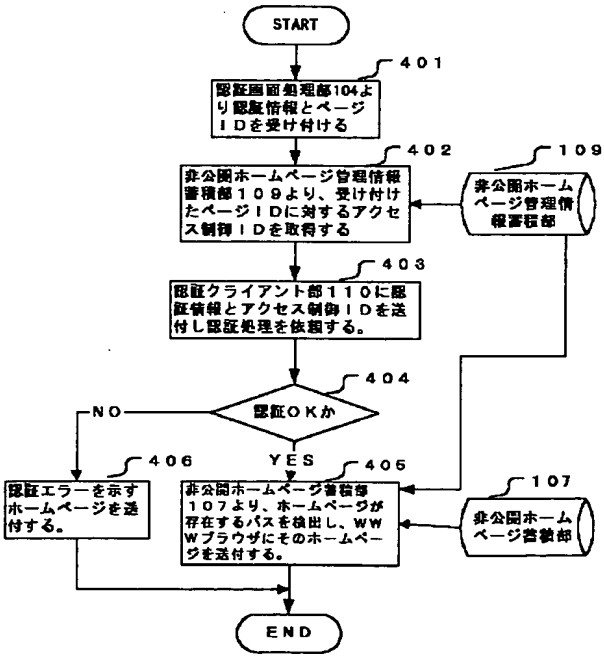
【図１】



【図２】



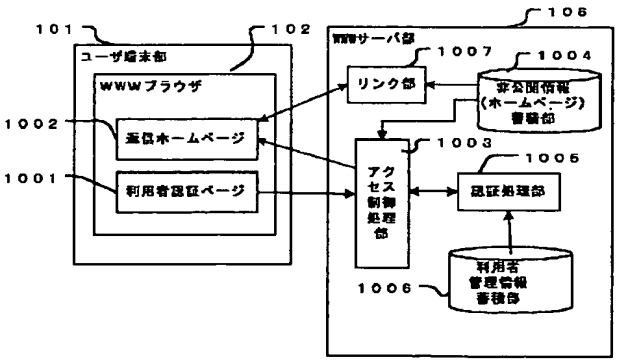
【図４】



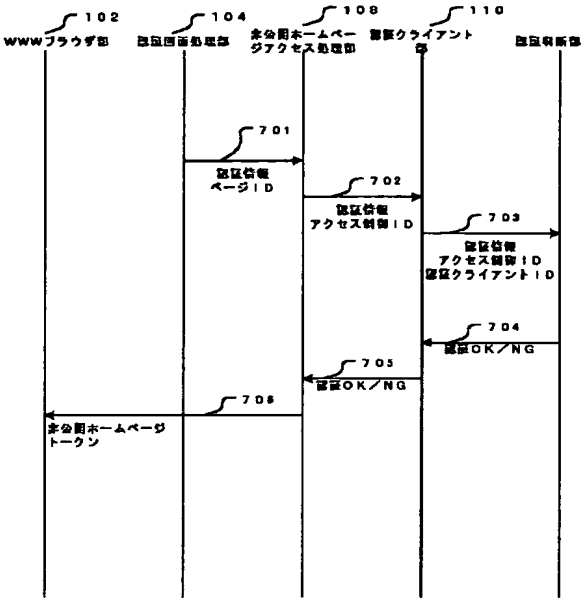
【図６】

601 ユーザID	602 認証クライアントID	603 アクセス制御ID	604 認証手段	605 備考
user1	AClient	JINJI1	ユーザIDと指紋情報１本	
user1	AClient	KEIRI1	ユーザIDとパスワード	

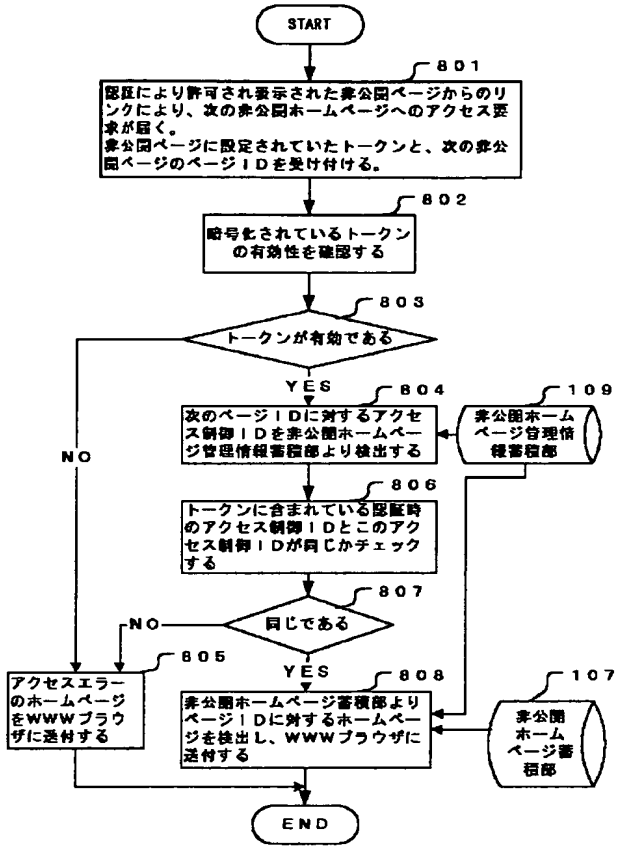
【図１０】



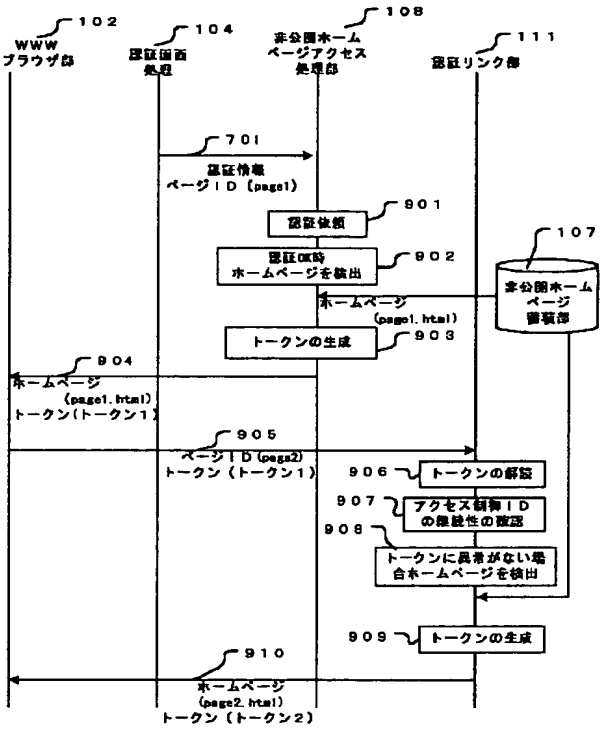
【図７】


102
WWWブラウザ部
104
認証画面処理部
106
非公開ホームページアクセス処理部
110
認証クライアント部
認証有効部
701
認証情報
ページＩＤ
702
認証情報
アクセス制御ＩＤ
703
認証情報
アクセス制御ＩＤ
認証クライアントＩＤ
704
認証ＯＫ／ＮＧ
705
認証ＯＫ／ＮＧ
706
非公開ホームページ
トークン

【図８】


START
801
認証により許可され表示された非公開ページからのリンクにより、次の非公開ホームページへのアクセス要求が届く。
非公開ページに設定されていたトークンと、次の非公開ページのページＩＤを受け付ける。
802
暗号化されているトークンの有効性を確認する
803
トークンが有効である
YES
NO
804
次のページＩＤに対するアクセス制御ＩＤを非公開ホームページ管理情報蓄積部より検出する
109
非公開ホームページ管理情報蓄積部
806
トークンに含まれている認証時のアクセス制御ＩＤとこのアクセス制御ＩＤが同じかチェックする
807
同じである
NO
YES
805
アクセスエラーのホームページをWWWブラウザに送付する
808
非公開ホームページ蓄積部よりページＩＤに対するホームページを検出し、WWWブラウザに送付する
107
非公開ホームページ蓄積部
END

【図９】



フロントページの続き

(72)発明者　貞包　哲男
東京都千代田区丸の内二丁目２番３号　三
菱電機株式会社内

Ｆターム(参考)　5B085 AE04 AE06 AE23 BG07